David M. Berger (SBN 277526)
**GIBBS LAW GROUP LLP**
1111 Broadway, Suite 2100
Oakland, California 94607
Telephone: (510) 350-9713
Facsimile: (510) 350-9701
dmb@classlawgroup.com

Norman E. Siegel (*pro hac vice*)
J. Austin Moore (*pro hac vice*)
Kasey Youngentob (*pro hac vice*)
**STUEVE SIEGEL HANSON LLP**
460 Nichols Road, Suite 200
Kansas City, Missouri 64112
(816) 714-7100 (tel.)
siegel@stuevesiegel.com
moore@stuevesiegel.com
youngentob@stuevesiegel.com

*Attorneys for Plaintiffs*

UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

| | |
|---|---|
| ABBY LINEBERRY, TERRY MICHAEL COOK, and MIGUEL CORDERO, individually and on behalf of all others similarly situated,<br><br>Plaintiff,<br><br>v.<br><br>ADDSHOPPERS, INC. and PEET'S COFFEE, INC.<br><br>Defendants. | Case No. 3:23-cv-01996-VC<br><br>FIRST AMENDED CLASS ACTION COMPLAINT<br><br>JURY TRIAL DEMANDED |

**FIRST AMENDED CLASS ACTION COMPLAINT**

Plaintiffs Abby Lineberry, Terry Michael Cook, and Miguel Cordero ("Plaintiffs") bring this class action complaint against AddShoppers, Inc., d/b/a SafeOpt; and Peet's Coffee, Inc. ("Peet's") (collectively "Defendants"), on behalf of themselves and all others similarly situated. Plaintiffs make these allegations based on personal knowledge as to their own actions and upon information and belief as to all other matters.

## NATURE OF THE ACTION

1. Imagine surfing the web and stumbling upon a retailer's website. You view an item and then leave the website without creating an account or providing any personal information. Later that day, you receive an email to your personal email account on behalf of the retailer imploring you to return to the website and purchase the product. But you never gave the retailer your email address. In fact, you never gave the retailer any of your personal information. So how did it get access to your browsing history and personal contact information? The answer is illicit web tracking by a marketing company known as AddShoppers.

2. AddShoppers runs a marketing enterprise that illicitly tracks persons across the internet, collects their personal information without consent, and then uses that information to send direct solicitations—all unbeknownst to the individual. So, for example, if a person creates an account to purchase pet food on a retailer's website, and the retailer is part of the AddShoppers "Data Co-Op", AddShoppers surreptitiously captures the information provided to the retailer, tracks the person's web browsing across the internet, and then uses their information to provide targeted advertisements to the individual on behalf of members of the Data Co-Op.

3. AddShoppers calls its "marketing" program "SafeOpt." It markets SafeOpt as a service consumers can voluntarily opt into to "receive verified offers from SafeOpt's brand partners." But the reality is very few individuals voluntarily opt into this program. Instead, they are unwittingly captured in it when they create an account and make a purchase on a website that—unbeknownst to them—is part of the AddShoppers' Data Co-Op. As the Data Co-Op grows, so does its dossier on unconsenting targets. Of course, AddShoppers has a financial incentive to market this way: it takes a cut of every purchase made via an unauthorized solicitation.

4. Hundreds of individuals have complained online about receiving targeted emails from retailers "via SafeOpt" who they never provided with their personal information. "*Creepy*", "*sleazy*", "*disgusting advertising*", "*unethical*", and an "*invasion of privacy*" are just a few snippets of the public commentary condemning this unconsented and ultra-invasive marketing practice.

5. It is also illegal. AddShoppers and members of the Data Co-Op are violating California's statutory consumer protection laws, and common laws intended to protect individuals' privacy rights. This case seeks redress for these violations.

## PARTIES

6. Plaintiff Abby Lineberry is a resident and domiciliary of Fontana, California.

7. Plaintiff Terry Michael Cook is a resident and domiciliary of Seminole, Florida.

8. Plaintiff Miguel Cordero is a resident and domiciliary of Sacramento, California.

9. Defendant AddShoppers, Inc. is a Delaware corporation with its principal place of business at 15806 Brookway Dr. Suite 200, Huntersville, NC 28078. AddShoppers does business throughout California and the entire United States.

10. Defendant Peet's Coffee, Inc. is a Virginia corporation with its principal place of business at 1400 Park Avenue, Emeryville, California 94608. Peet's does business throughout California and the entire United States and participates as a member of AddShoppers' Data Co-Op.

**JURISDICTION AND VENUE**

11. This Court has subject matter jurisdiction over this lawsuit under the Class Action Fairness Act, 28 U.S.C. § 1332(d), because this is a proposed class action in which: (1) there are at least 100 class members; (2) the combined claims of class members exceed $5,000,000.00, exclusive of interest, attorneys' fees, and costs; and (3) Defendants and at least one class member are citizens of different states.

12. This Court has general personal jurisdiction over Peet's and Presidio Brands because they are headquartered in this State.

13. This Court has personal jurisdiction over AddShoppers because it has purposefully availed itself of the laws and benefits of doing business in this State, and Plaintiffs' claims arise out of each of the AddShoppers' forum-related activities. AddShoppers intentionally installed the wiretaps at issue. It purposefully intercepted electronic transmissions from users of the websites. The conduct also was expressly aimed at California residents. AddShoppers knew that a significant number of Californians would visit its partner websites because they form a significant portion of both companies' target market. By intercepting the transmissions of the websites' users, AddShoppers targeted their wrongful conduct at customers they knew were residents of California. It was foreseeable that Defendants' interceptions and wiretapping would harm Plaintiffs and similarly situated individuals who resided in California.

14. AddShoppers also specifically advertises its alleged compliance with California's privacy laws to prospective partners. It already partners with hundreds of California companies' websites. And it sends thousands (if not millions) of targeted emails to Californians. Simply put, a substantial portion of the events giving rise to Plaintiffs' claims occurred in this District.

15. Venue is proper in this District because a substantial part of the events or omissions giving rise to the claim occurred in this District.

## STATEMENT OF FACTS

### A. SafeOpt: Track and Conquer

16. AddShoppers advertises its SafeOpt service two ways: one is to shoppers, and another is to businesses.

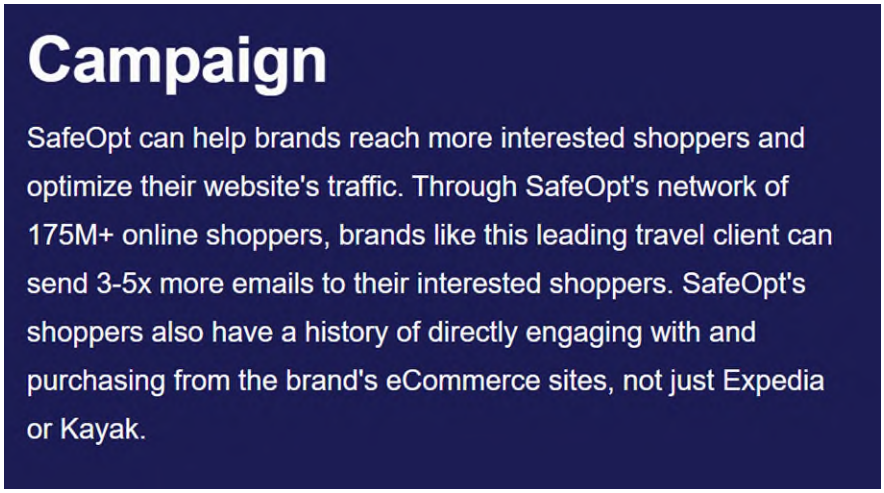
17. To shoppers, SafeOpt is held out as "free service that sends you Verified Offers while you shop from thousands of participating brands to help save you time & money. We've designed SafeOpt® to protect your data and give you control over your information."[1]

18. To the few people that opt into the service, AddShoppers says: "When you enter your email and join SafeOpt®, our technology makes note of the device you're using and generates a secure anonymous ID. When one of our brand partners that also has our technology installed on their website sees your device, they know to show your ID promotions and offers not generally available to the broader public. No more (expired!) promo code hunting and things to install -- just a seamless shopping experience with delightful surprises for you!"[2]

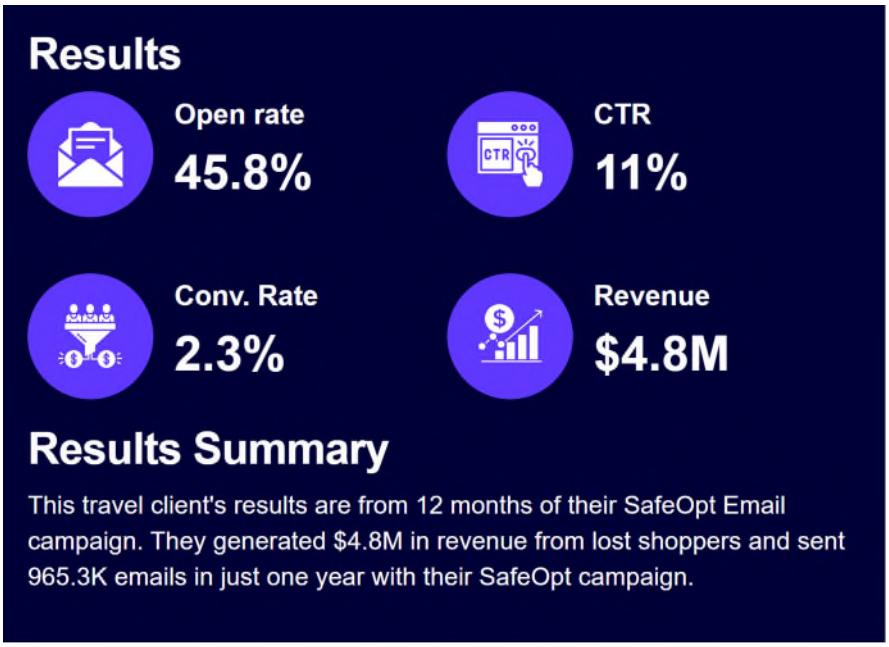
[1] *SafeOpt Homepage*, available at https://www.safeopt.com/ (last visited April 14, 2023).
[2] *SafeOpt Frequently Asked Questions*, available at https://www.safeopt.com/ (last visited April 14, 2023).

19. To businesses, AddShoppers claims SafeOpt offers the opportunity to "send 3-5x more emails to shoppers who abandon your website" by "using our list of 175M+ U.S. shoppers."[3]

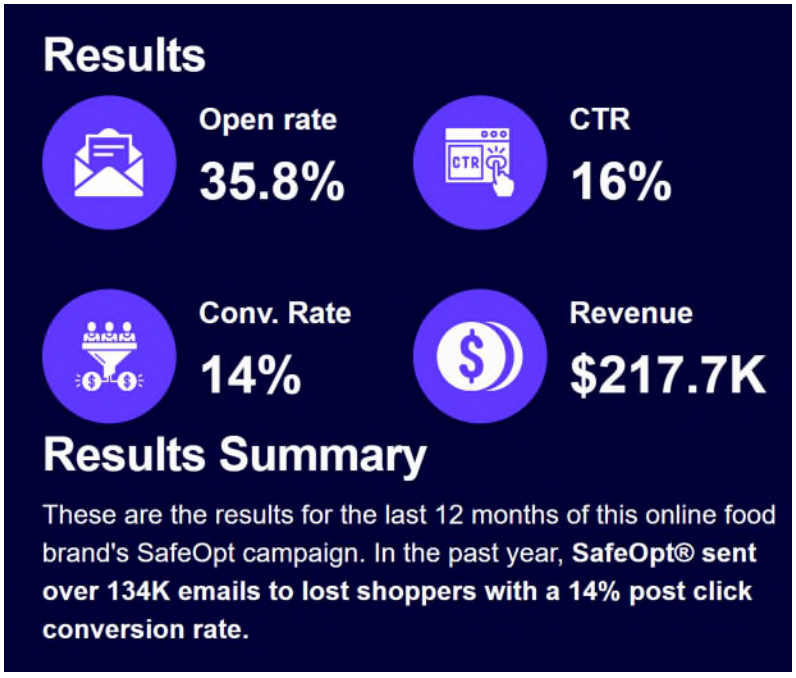
20. The SafeOpt website provides case studies for various industries touting the success of its "track and conquer" program. For example, it states that: "This travel client's results are from 12 months of their SafeOpt Email campaign. They generated $4.8M in revenue from lost shoppers and sent 965.3K emails in just one year with their SafeOpt campaign."

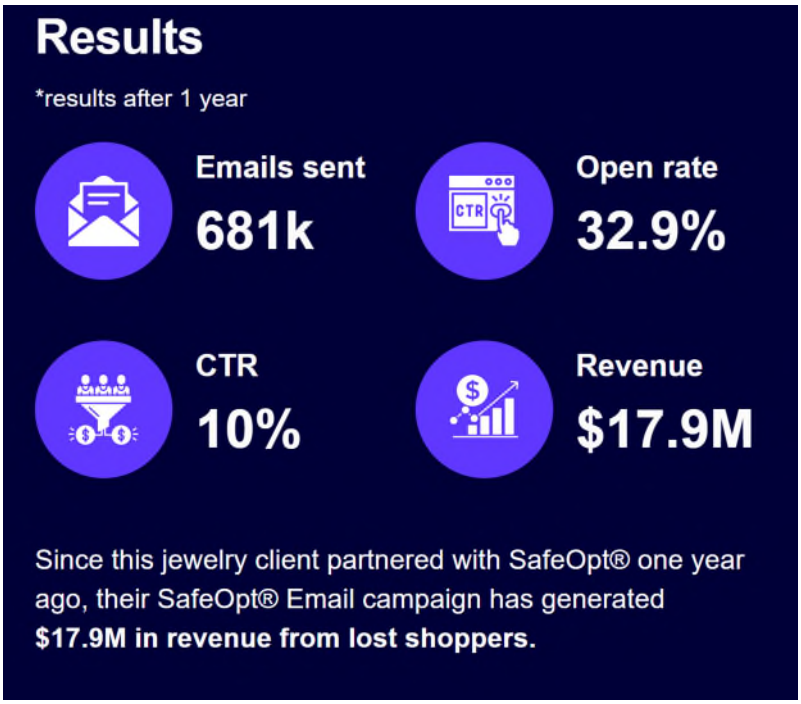



[3] *SafeOpt by AddShoppers Intro*, available at https://calendly.com/d/cft-zy7-gz2/safeopt-intro?month=2022-11 (last visited April 14, 2023).




21. For a food and beverage client, SafeOpt touted sending 134,000 emails over a 12-month period "to lost shoppers with a 14% post click conversion rate." For a jewelry client, SafeOpt sent 681,000 emails over a 12-month period, resulting in $17.9 million in additional revenue.






22. AddShoppers touts SafeOpt's "network with 2,000+ large brands and publishers" including companies like Everlast, Maui Jim, Blue Nile, Sierra, Warby Parker, Gopuff, Nutrisystem, and Goop.

**B. SafeOpt: The Wiretapper**

23. While AddShoppers paints a benevolent picture of SafeOpt's advertising prowess, the terms and conditions AddShoppers imposes on its partner business detail a much more invasive and sinister operation.

24. AddShoppers requires its partner brands to share their "User Data" with AddShoppers, which includes "data collected by SafeOpt technology … related to such Authorized

Users' web browsing as a result of services rendered to you, as well as user opt-in consent to share the User Data with SafeOpt."[4]

25. AddShoppers further requires participation in a "Data Co-op" which permits SafeOpt to "leverage[] a shared pool of user data collected by SafeOpt technology" by granting "SafeOpt with a limited, transferable license to their User Data for the purpose of providing identity resolution and direct messaging services for each Data Co-op member's audience."[5]

26. AddShoppers' terms also permit it to collect all "Client Data" derived from its partner companies, including their customers' User Data, and states that "SafeOpt may exploit Client Data for any lawful purpose without any duty of accounting or compensation to you."[6]

27. And exploit it does. AddShoppers surreptitiously collects and pools the sensitive personal information provided by individuals to online retailers in confidence, creates dossiers on those individuals, and then tracks them across the internet to monitor their web browsing for its own financial benefit.

28. While AddShoppers' terms and conditions reference being granted a license to collect the personal information of its partner companies' customers (what AddShoppers defines as "authorized users")—the reality is the *users themselves* never authorized their data to be shared this way. Indeed, they had no idea that while buying a product their information was surreptitiously being transmitted to a company granting itself free rein to "exploit" their information as it chooses.

---

[4] *SafeOpt Terms of Use Effective Date: May 12, 2021*, available at https://www.safeopt.com/terms (last visited April 14, 2023).
[5] *Id*. at Data Co-Op.
[6] *Id*. at Client Data.

29. In an interview about its business, AddShoppers co-founder Chad Ledford described the operation of the Data Co-Cop as follows:

> [Chad Ledford]: Yeah, so there's kind of two data sources that we have. One is a blind Co-Op, which I would say half of our clients are participating in that, and the blind Co-Op is the brands submitting data into it in exchange for being able to use the data that comes out of it to activate the campaigns. We don't sync data, we don't actually put data into another system, it's all self-contained within our system, but about half of the volume that we see comes from that Co-Op of data.
>
> And then the other half comes from publisher relationships that we have where we license the data, and again, we don't sell data, or we don't push data out of it so that users can still control all their data, but it gives us additional scale so that we can start to match who these people are.
>
> [Interview host]: That's awesome. Was there any hesitancy with the brands sharing their data initially, or is it a little bit easier once they heard that other brands you were working with were already doing that?
>
> [Chad Ledford]: Yeah, we offer both. If they want access to the Co-Op data, they have to be part of it, so they have to submit to get access to it, that's basically what makes it the Co-Op. So, they can still work with us, and they can still tap into that publisher data, and **a lot of the enterprise brands that we work with will never submit any data to any other system including us, and it's just off the table, it's not going to get through legal.** We can still work with those brands, we just do it through our licensed publisher data. But the thing that gets us really excited is that idea of the Co-Op, and the brands being able to work together to do more together.[7]

30. In other words, AddShoppers operates a "data lake" where it collects as much information relating to a user as possible all from different sources, stores that information in a centralized location where it matches data points and creates detailed profiles on individuals, and then uses those profiles to send direct, targeted advertisements from Co-Op companies even when the user did not authorize it. Ledford suggested that the company intends to collect and utilize even

[7] Mission.org Podcast, *Diversifying To Become Future-Proof with Chad Ledford, Co-Founder of AddShoppers*, https://mission.org/up-next-in-commerce/diversifying-to-become-future-proof-with-chad-ledford-co-founder-of-addshoppers/ (emphasis added).

more personal information like "gender data" and "demographic data" as the company continues to grow.[8]

31. Central to AddShoppers' data collection operation is its use of malicious, third-party tracking cookies. Cookies are small text files that are stored on a user's computer or mobile device by a website. They are used to save information about the user's browsing activity, such as login information, shopping cart contents, and browsing history.[9]

32. But not all cookies are created equal. A first-party cookie is created and stored by the website the user is visiting, also known as the host domain. It allows the website to collect customer analytics data, remember language settings, and carry out other useful functions that help provide a positive user experience. This means the browser can remember key pieces of information, such as items added to shopping carts, username and passwords, and language preferences. These are generally considered necessary and helpful cookies.[10]

33. Third-party cookies, by contrast, are those created by domains other than the one the user is visiting. These cookies are accessible on any website that loads the third-party server's code. Because they can be accessed by multiple domains, third-party cookies can be used to track a user's browsing activity across multiple websites.

34. Companies that join the Co-Op agree to install AddShoppers' code on their website. When an internet user creates an account or makes a purchase with the business, a third-party tracking cookie is created that includes a unique value AddShoppers associates with that user. The

---

[8] *See id*.

[9] Cloudfare, *What are cookies*, available at: https://www.cloudflare.com/learning/privacy/what-are-cookies/.

[10] Clearcode, *What's the Difference Between First-Party and Third-Party Cookies*?, available at https://clearcode.cc/blog/difference-between-first-party-third-party-cookies/#first-party-cookies.

cookie is hidden on the user's browser and automatically sends information to AddShoppers' SafeOpt domain "shop.pe." AddShoppers then associates that unique value with the personal information the user provided to the company, which typically includes, at a minimum, full name, address, payment card information, and email address.

35. With the tracking cookie hidden in the user's browser, AddShoppers can monitor the user's browsing activity across the internet. If the user lands on another website in the SafeOpt network, the cookie values "sync" and AddShoppers tracks the user's activity on the website, including the user's detailed referrer Uniform Resource Locator ("URL"). Because AddShoppers already associates personal information with the cookie value, it can directly advertise to the user even where the user leaves a website without affirmatively providing any personal information.

36. While companies often use "browser-abandonment" emails to encourage customers to return to their website and purchase a product they put in their cart but never purchased, the companies do so for users who have *already provided the company with their email address*. Likewise, when marketing companies use "cookie synching" to provide targeted advertisements (think searching online for a pair of shoes and later seeing those shows in an advertisement on your browser), the cookie value they use is an anonymized identification number that is not associated with any personally identifiable information ("PII") tied back to the user.

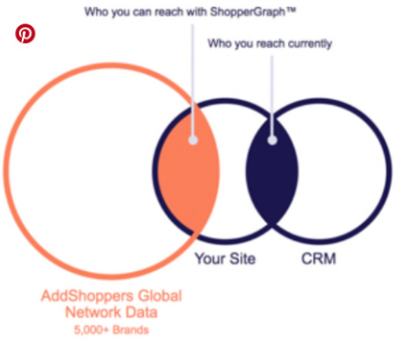
37. AddShoppers, by contract, *intentionally associates* PII with the unique cookie value assigned by AddShoppers, the basis for its entire business model. In fact, in a now deleted blog post, AddShoppers describes its use of unsolicited, targeted emails to increase sales:

> Send 2x-5x more personalized triggered emails with incremental campaigns.
>
> The Problem Marketers are unable to send email reliably to customers that have not provided their email previously. This means more than 95% of your web visitors cannot receive a relevant email from you.

**The Solution** Connecting the AddShoppers network of 150M+ shoppers through its Email Retargeting® Co-op, marketers are able to resolve identities and deliver 1:1 email regardless of customer email acquisition.

**How it works** Today, if 100 customers visited your website — between your ESP [email service provider], CRM [customer relationship management], and other platforms — you might be able to send a browse abandon or cart abandon email to 4-5 of those site visitors. What about the other 95 visitors? Without AddShoppers your only option is retargeting ads, which continue to get more and more expensive.

With AddShoppers, our system will attempt to match the 95 visitors in real-time against our network of 150M+ monthly profiles and 5,000+ websites. If the visitor leaves your site without signing up for email or buying AND we find a match, AddShoppers will enable a triggered email sequence to help you win back those customers and engage them in a way you can't today.





**Browse + Product Abandon Reminders** A customer is shopping in your catalog as a guest (no sign-in required) and leaves the site without adding a product to shopping cart. Send them the products or content they were looking at directly to their inbox. This typically doubles the performance you're getting from dynamic retargeting ads.

**Active Cart Abandon Reminders** A customer is shopping on a website as a guest and leaves the cart without checking out. With our email retargeting, the marketer can send a personalized and timely communication to the consumer in a more direct medium, redirecting the consumer back to the site to complete the purchase.[11]

[11] *Wayback Machine Screen Capture*, available at: https://web.archive.org/web/20200710211126/https://www.addshoppers.com/blog/email-retargeting-co-op.

38. AddShoppers co-founder Chad Ledford also confirmed in an interview that AddShoppers' business model hinges on its ability to send targeted emails to individuals who never voluntarily provided their email address to a member of the Data Co-Op:

> [Chad Ledford]: Yeah so, most digital commerce brands realize the value of email today, especially whenever it comes to retention and lifetime value. So, the conversations are a little bit easier now because they understand that it is a really strong channel, and it's one that they have to defend, but most brands can only tap into what's considered first party data. So, first party data is data that the brand captured themselves. So, a lot of people build up emails from popups, or they capture it during the checkout process or things like that, but that usually ends up being anywhere from like three to 5% of their traffic that they've spent a lot of money to get to their site that they're actually able to capture, and be able to continue creating that relationship with them.
>
> **So, the problem that we help solve today is tapping into that other 95% of people that are on the website, people that haven't given them their email address yet, but they're still showing a lot of engagement, and they probably still want to try to get those people to be their customers**.
>
> [Interview host]: **Got it, so the people who are just casually browsing, or maybe added something to the cart and then left, the people like that who didn't directly give the brand their email, but maybe seemed kind of interested**.
>
> [Chad Ledford]: **Yep, exactly**.[12]

39. AddShoppers typically solicits in the form of a direct email from the retailer "via SafeOpt" imploring a user to return to the website to purchase a product they were looking at, even though the individual never gave their email address to the retailer or authorized such communications. Of course, AddShoppers does this with a pure profit motive as it takes a cut of all sales made "via affiliate links in emails, texts, apps, and content."[13]

---

[12] Mission.org Podcast, *Diversifying To Become Future-Proof with Chad Ledford, Co-Founder of AddShoppers*, https://mission.org/up-next-in-commerce/diversifying-to-become-future-proof-with-chad-ledford-co-founder-of-addshoppers/ (emphasis added).

[13] https://www.safeopt.com/learn/email-retargeting-strategies-for-ecommerce-brands

40. A software engineer who authored a blog post criticizing AddShoppers' marketing practices offered the following analogy: "Imagine if every store you visited would take a picture of you and then share and compare it with neighboring stores until they find one that you are a customer of and has your information. If such an agreement was in place, that store would now share who you are with the store that you are not yet a customer of and then add you to their marketing list. This is exactly what 'AddShoppers' does."[14]

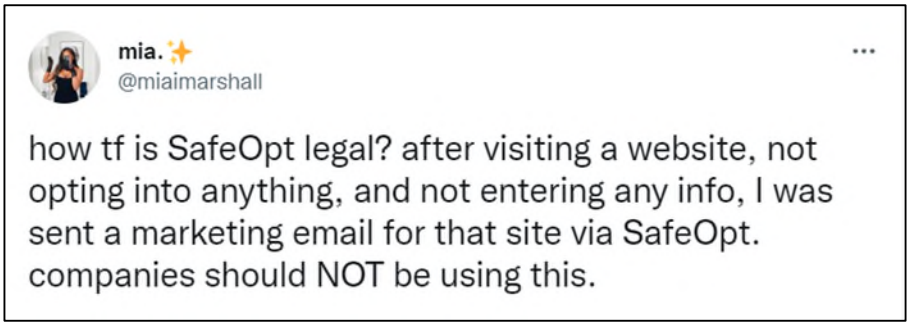
41. AddShoppers' illicit tracking practices have been broadly condemned. Below are just a small sample of user complaints over the company's privacy practices.


[14] Heshie Brody, *I Was Emailed after Abandoning a Registration Form. I Did Not Click Submit. This Is Not Ok* (June 1, 2020), available at: https://dev.to/heshiebee/i-was-emailed-after-abandoning-a-registration-form-i-did-not-click-submit-this-is-not-ok-a63.

Jay | Gay | Shirtless everyday
@shirtlessjay

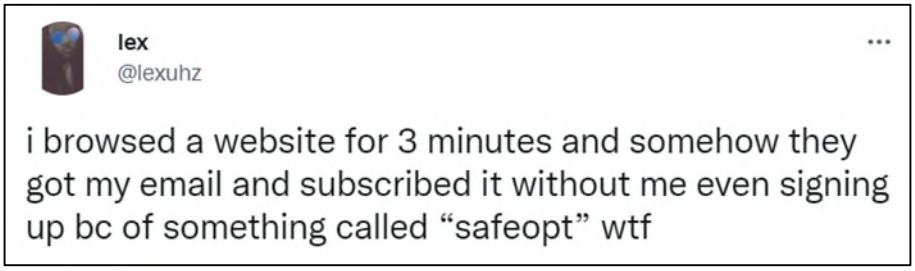
Was looking into webcam I heard about, browsed a site for a minute, never gave my email, and never put anything in my cart. Two minutes later, I get this email.

I had never heard of SafeOpt before, but let me tell you, if you want me to NEVER buy your product, do this bullshit.



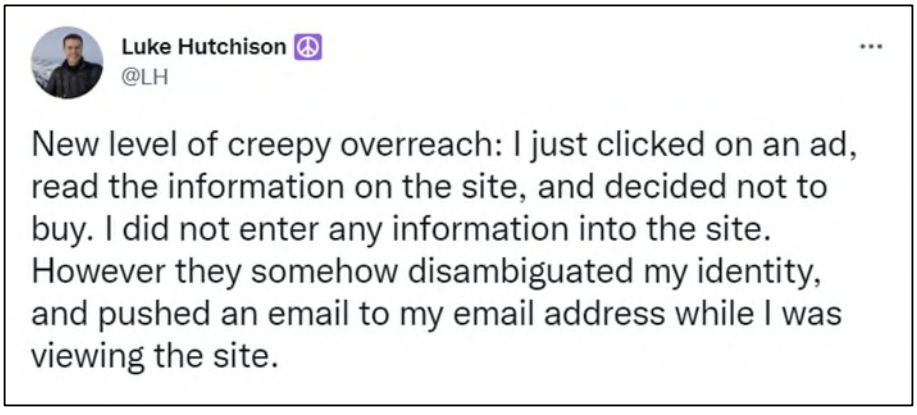
mia. ✨
@miaimarshall

how tf is SafeOpt legal? after visiting a website, not opting into anything, and not entering any info, I was sent a marketing email for that site via SafeOpt. companies should NOT be using this.



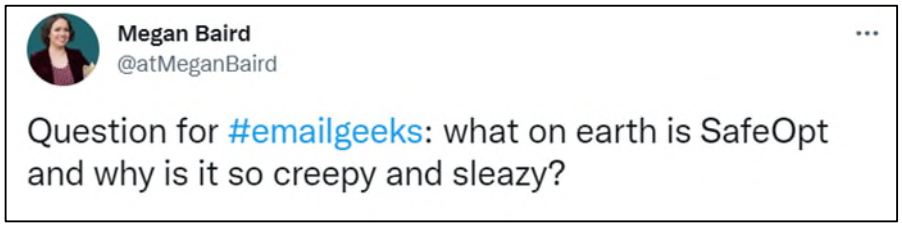
lex
@lexuhz

i browsed a website for 3 minutes and somehow they got my email and subscribed it without me even signing up bc of something called “safeopt” wtf

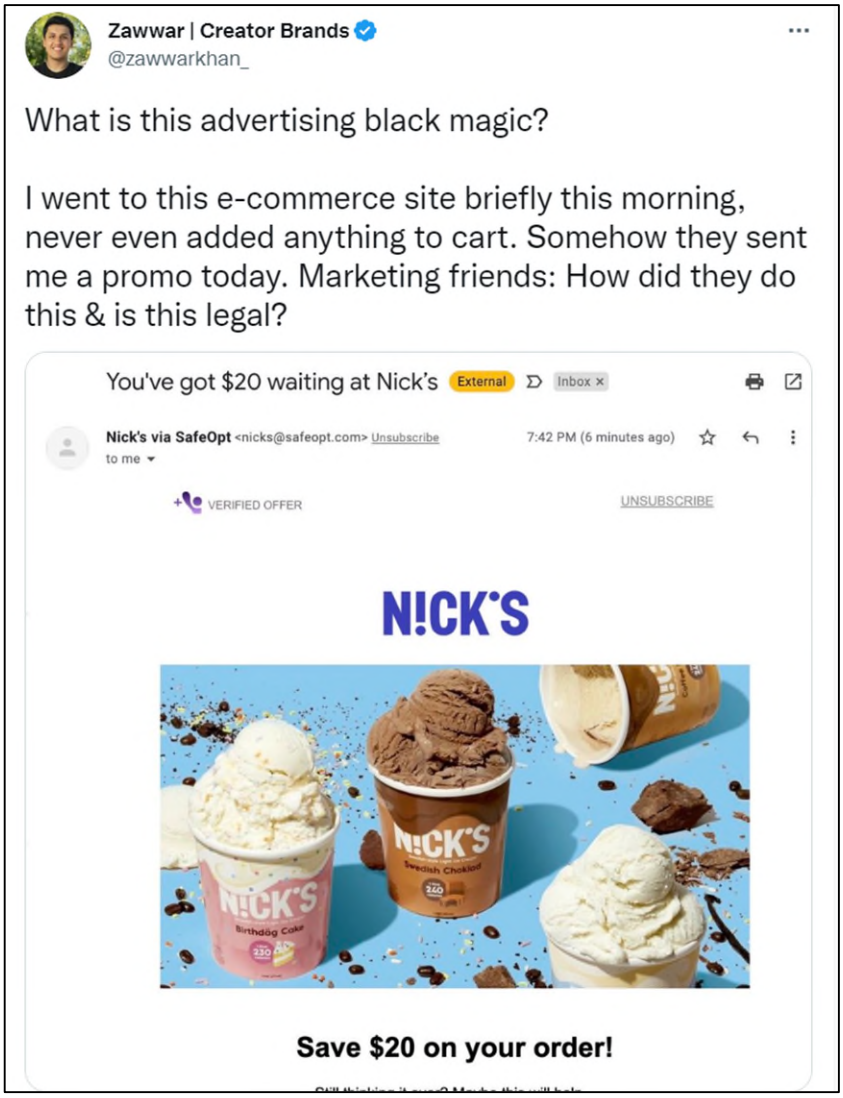


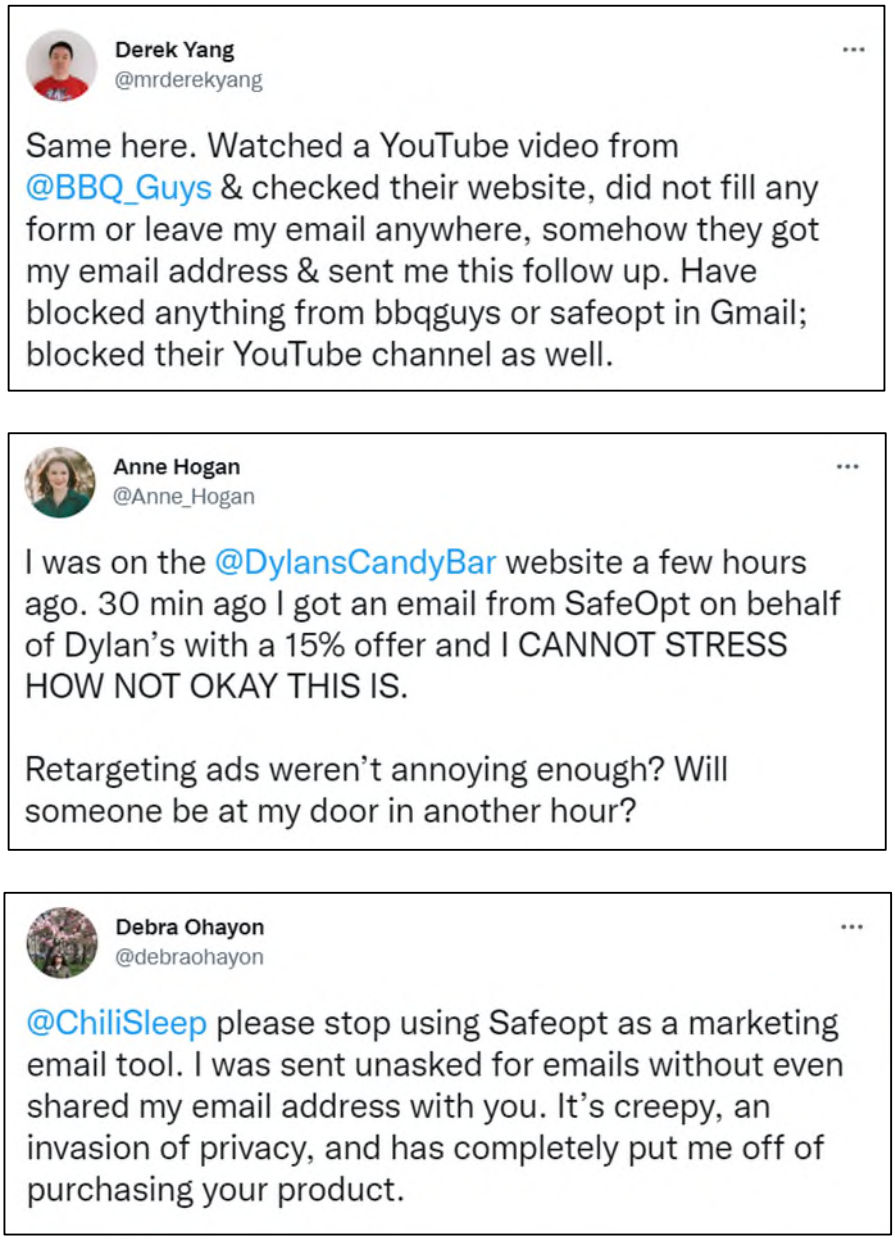
Luke Hutchison ☮
@LH

New level of creepy overreach: I just clicked on an ad, read the information on the site, and decided not to buy. I did not enter any information into the site. However they somehow disambiguated my identity, and pushed an email to my email address while I was viewing the site.


Megan Baird
@atMeganBaird
Question for #emailgeeks: what on earth is SafeOpt and why is it so creepy and sleazy?


Elizabeth Story
@HyperbolicTelly
SafeOpt is skeevy as hell and I just had to write a terse email to a company that I would not be buying anything due to their inbox creeping


Zawwar | Creator Brands
@zawwarkhan_
What is this advertising black magic?
I went to this e-commerce site briefly this morning, never even added anything to cart. Somehow they sent me a promo today. Marketing friends: How did they do this & is this legal?
You've got $20 waiting at Nick's
External
Inbox ×
Nick's via SafeOpt <nicks@safeopt.com> Unsubscribe
to me
7:42 PM (6 minutes ago)
VERIFIED OFFER
UNSUBSCRIBE
N!CK'S
Save $20 on your order!




42. AddShoppers' Better Business Bureau webpage is also flooded with complaints from individuals who received unsolicited email advertisements from SafeOpt.[15] For example, one review reads: "I understand what they are doing is 'legal' but it is shady and misleading. I received

[15] *See Better Business Bureau Customer Reviews, AddShoppers*, available at: https://www.bbb.org/us/nc/huntersville/profile/digital-marketing/addshoppers-0473-307901/customer-reviews (last visited April 14, 2023).

a marketing re-targeting email from a company I never gave my email to and saw it was connected to 'SafeOpt' (another purposefully misleading name to include the word 'safe'). I should have control over who has my email. It should not be possible to opt into SafeOpt's ENTIRE NETWORK OF ADVERTISERS just by opting in on ONE of them. Brands should be ashamed to use this service, it is bad for my personal data and it is bad for data security."

43. AddShoppers' standard response to these complaints is to place blame on partner members of the Data Co-Op ("*We emailed on behalf of the sites you visited shown in the email. That was based on the [partner] site[']s settings and its privacy policy*"); refer to its tracking as industry standard ("*Many websites review who[']s visiting, and try to engage with visitors*"); and encourage the use of privacy technology to block SafeOpt's *own* tracking cookies ("*Consider using a VPN + adjusting your browser settings for more anonymity online*.").[16]

**AddShoppers Response** 11/08/2022

We emailed on behalf of the sites you visited shown in the email. That was based on the sites settings and its privacy policy. The emails are intended to be helpful (i.e., provide site offers, discounts, etc.), but the email address you provided has now been unsubscribed. Many websites review whos visiting, and try to engage with visitors. Consider using a VPN + adjusting your browser settings for more anonymity online.

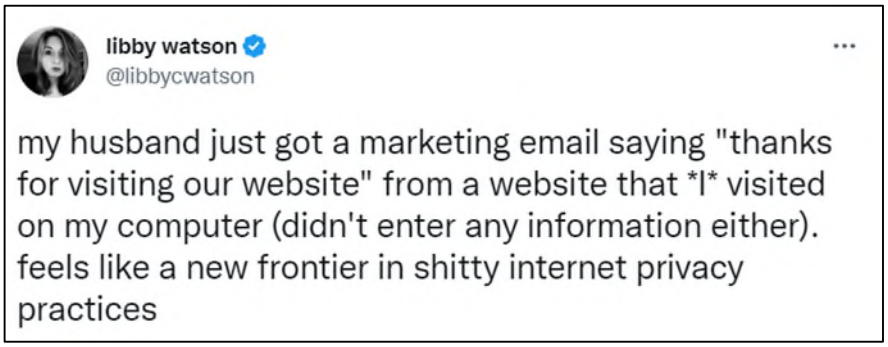
44. The consequences of this type of tracking are serious. Among many other privacy concerns, SafeOpt's network of businesses includes companies that sell highly personal products, including feminine hygiene and men's health products. As a result, SafeOpt can reveal exceptionally private information about customers to anyone that shares a computer. The software engineer who authored the blog post criticizing AddShoppers noted that he received an email to

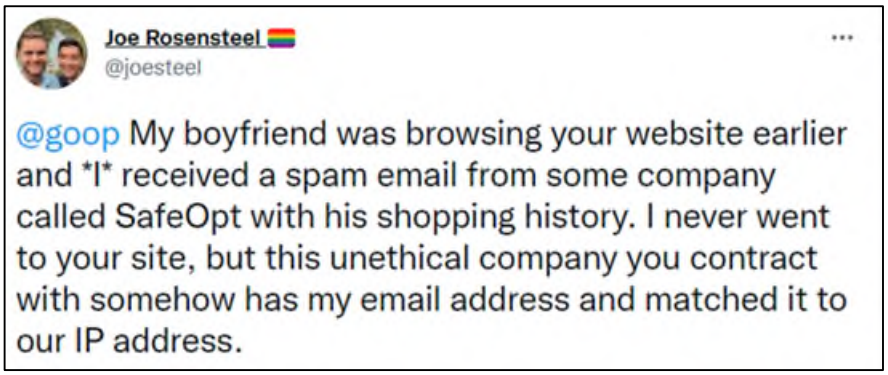
[16] "VPN" stands for "virtual private network" which is a service that encrypts a user's activity on the internet and keeps their identity hidden while browsing.

his personal account imploring him to return to purchase a breast pump even though he never provided his information to the website.[17] Another internet user received emails from a colon cleansing company after he visited the website without providing any personal information.


45. Other victims report having received unsolicited emails revealing their *partner's* browsing history or had their personal browser history sent to their *work* email address.

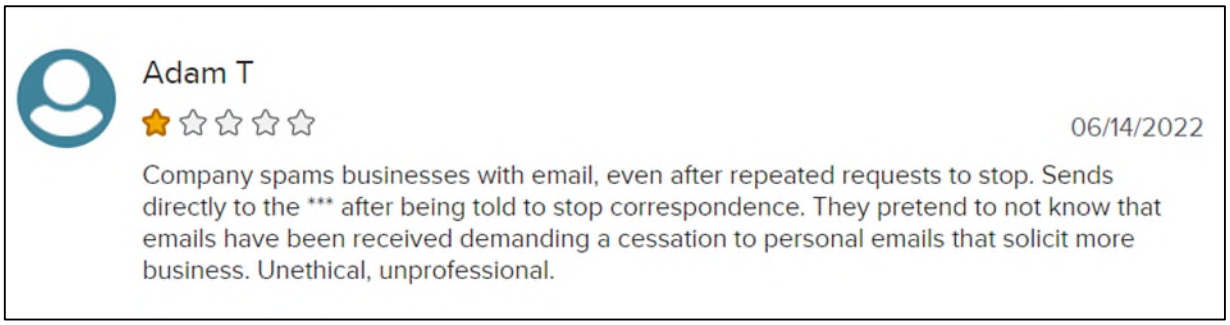
[17] Heshie Brody, *I Was Emailed after Abandoning a Registration Form. I Did Not Click Submit. This Is Not Ok* (June 1, 2020), available at: https://dev.to/heshiebee/i-was-emailed-after-abandoning-a-registration-form-i-did-not-click-submit-this-is-not-ok-a63.



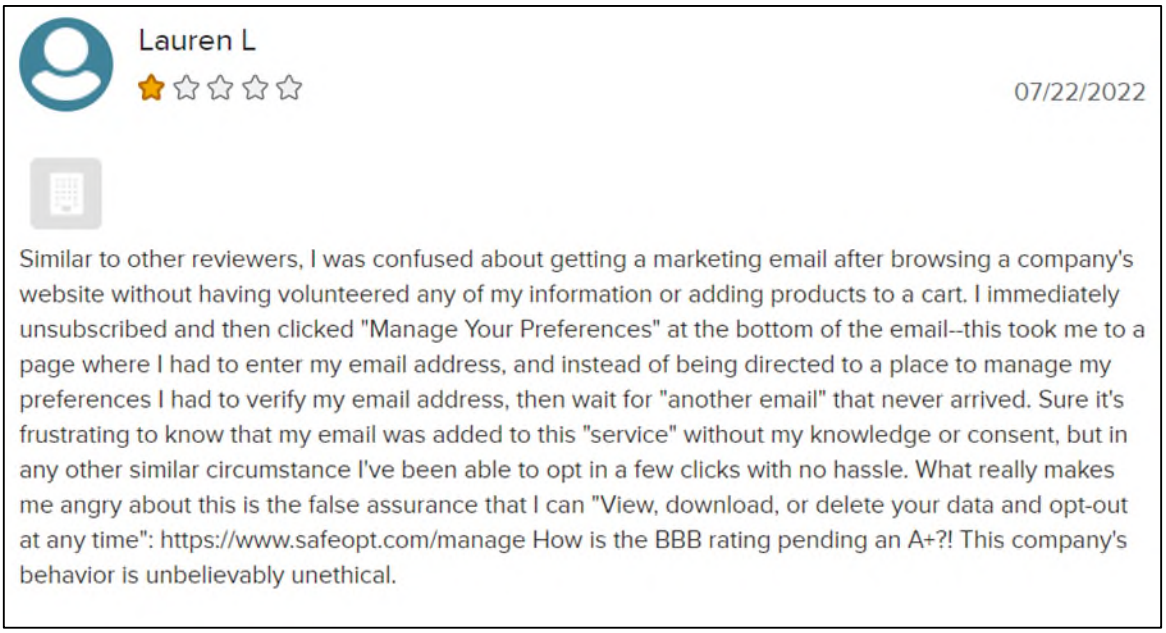



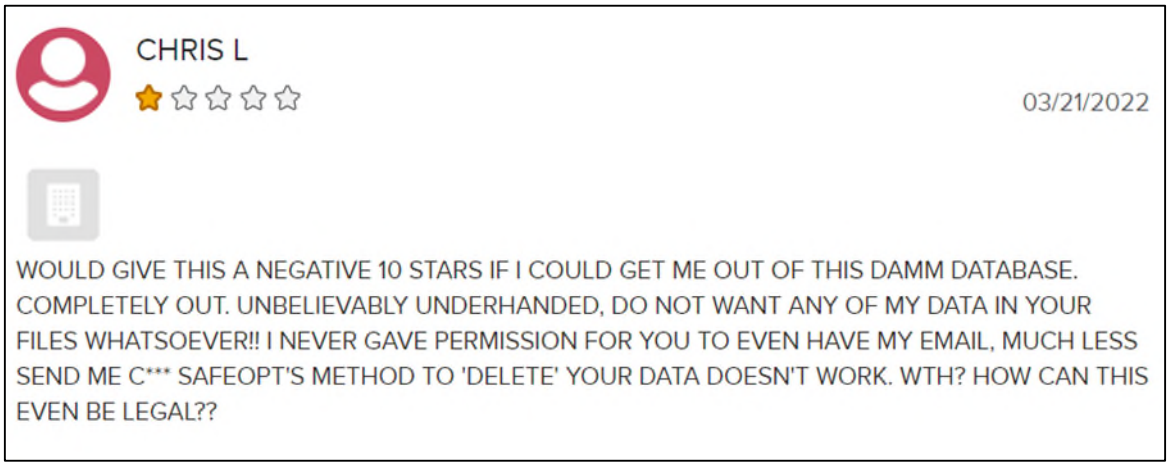


46. When users receive an email from a retailer "via SafeOpt"—they are purportedly given the option to unsubscribe from such emails (even though they never subscribed to begin with). However, when users try to do so, they are not actually removed from the SafeOpt network and continue to receive marketing emails from AddShoppers.


47. When individuals go directly to SafeOpt's website and attempt to opt-out or delete their data, they are met with similar resistance.






48. Under the California Consumer Privacy Act, businesses like AddShoppers are required to disclose what personal information they collect and share about California citizens. Specifically, California citizens can request: (1) the categories of personal information collected; (2) specific pieces of personal information collected; (3) the categories of sources from which the business collected personal information; (4) the purposes for which the business uses the personal information; (5) the categories of third parties with whom the business shares the personal information; and (6) the categories of information that the business sells or discloses to third parties. *See* Cal. Civ. Code § 1798.110.

49. But upon formal request, AddShoppers refuses to provide this information. Instead, it simply directs those inquiring to a general disclosure in its privacy policy stating that it collects every type of data imaginable.

50. Thus, AddShoppers refuses to abide by opt-out requests and refuses to disclose on an individual-level basis what information it collects and who receives it. When individuals try to request a download file of their data from AddShoppers, they are sent a text file that may include their email address and certain Co-Op websites' time stamps but omits the vast amount of additional information AddShoppers collects. Consequently, even after users learn their data is

being misused by AddShoppers, they still have no recourse to learn how AddShoppers used it historically and will use it going forward.

51. AddShoppers' prized list of hundreds of millions of U.S. shoppers[18] was not gained through voluntarily consent. Unwittingly, shoppers become part of AddShoppers' SafeOpt network without ever signing up for the service; instead, "joining" SafeOpt by making a purchase from a company participating in AddShoppers' Data Co-Op and having their information traded without their knowledge and consent.

52. Not only are AddShoppers' marketing and tracking practices unsavory, but they are also illegal. As deployed, AddShoppers' tracking software functions as a wiretap.

***Plaintiff Abby Lineberry***

53. On January 17, 2023, Plaintiff Lineberry visited medterrahemp.org, on her work computer, for her job as Supervising Food Safety Inspector at the California Department of Public Health. During her visit, she clicked on and reviewed some of medterra's CBD products. Plaintiff Lineberry had never visited medterrahemp.org before and never provided any personal information to the company.

54. During that visit, SafeOpt tracked Plaintiff Lineberry's precise webpage visit, including the items she viewed.

55. Although Plaintiff Lineberry cannot even access her personal email on her work computer, she later received an email to her personal email account from "medterrahemp.com via

[18] AddShoppers has recently claimed that has a "growing list of 250 million online shoppers and over 15,000 merchant brands."

SafeOpt" email account medterrahemp@mail.safeopt.com. The email included pictures of CBD gummies that Plaintiff Lineberry had viewed on the website.

56. Plaintiff Lineberry was shocked that her work-related browsing history was being emailed to her personal email address by a company she never provided it to.

57. Prior to receiving this email, Plaintiff Lineberry never heard of SafeOpt and never agreed to provide AddShoppers her information for the company to "exploit" for its own financial benefit.

***Plaintiff Terry Michael Cook***

58. On March 3, 2023, Plaintiff Cook visited Peets.com. During his visit, he clicked on and reviewed some of Peet's products. Plaintiff Cook had never provided any personal information to the company, agreed to any terms on Peet's website, or clicked "accept" on Peet's cookie acceptance banner.

59. During that visit, SafeOpt tracked Plaintiff Cook's precise webpage visit, including the items exact coffee products that he had viewed.

60. Plaintiff Cook later received an email to his personal email account from peets@safeopt.com. The email included pictures of the coffee products that Plaintiff Cook had viewed on the website. He received a second email on March 5, 2023, about the same products via SafeOpt.

61. Plaintiff Cook was shocked that his personal browsing history was now being sent to him by a company he never provided his email address.

62. Prior to receiving this email, Plaintiff Cook never heard of SafeOpt and never agreed to provide AddShoppers his information for the company to "exploit" for its own financial benefit.

***Plaintiff Miguel Cordero***

63. Plaintiff Cordero requested his data associated with his Gmail account from AddShoppers on July 25, 2024, which shows he had been tracked by at least a dozen companies for several years, including the exact dates and times he visited other websites that (unbeknownst to him) were part of the AddShoppers network. One such website was Peet's, which surreptitiously captured information about Plaintiff Cordero's visit to its website on November 9, 2021. Although he never provided personal information (including his email) to Peet's, AddShoppers carefully tracked his visit to be included in the Data Co-Op.

```
peets_com:
  last visit: '2021-11-09T22:38:38.381000+00:00'
```

64. Plaintiff Cordero never agreed to the terms and conditions for AddShoppers, or Peet's. And as a matter of practice, Plaintiff Cordero declines cookie banners.

65. Plaintiff Cordero visited Peet's website while in California.

66. Plaintiff Cordero was not aware AddShoppers or Peet's was collecting his personal information at the time he visited the website. He did not know (nor could have known) AddShoppers tracked his visit on Peet's website until he received his data from AddShoppers.

67. Plaintiffs each had their PII collected by AddShoppers and their online internet browsing monitored and tracked by AddShoppers without their consent. Plaintiffs and class members each have an interest in controlling how their PII is used and shared. Their information has independent value, which is recognized by AddShoppers and members of the Data Co-Op who

agree to collect and trade it for their personal gain. Plaintiffs and class members are harmed every time their PII is used or shared in a manner to which they did not consent, particularly when it is used to solicit them for marketing and advertising purposes.

68. Plaintiffs and class members seek to recover the value of the unauthorized access to their PII resulting from Defendants' wrongful conduct. This measure of damages is analogous to the remedies for unauthorized use of intellectual property. Like a technology covered by a trade secret or patent, use or access to a person's personal information is non-rivalrous—the unauthorized use by another does not diminish the rights-holder's ability to practice the patented invention or use the trade-secret protected technology. Nevertheless, a plaintiff may generally recover the reasonable use value of the IP—*i.e.*, a "reasonable royalty" from an infringer. This is true even though the infringer's use did not interfere with the owner's own use (as in the case of a non-practicing patentee) and even though the owner would not have otherwise licensed such IP to the infringer. A similar royalty or license measure of damages is appropriate here under common law damages principles authorizing recovery of rental or use value. This measure is appropriate because (a) Plaintiffs and class members have a protectible property interest in their PII; (b) the minimum damages measure for the unauthorized use of personal property is its rental value; and (c) rental value is established with reference to market value, *i.e.*, evidence regarding the value of similar transactions.

## CLASS ACTION ALLEGATIONS

69. Plaintiffs repeat and reallege all preceding paragraphs.

70. Under Federal Rule of Civil Procedure 23, Plaintiffs assert claims on behalf themselves and the following proposed class and subclass:

> All persons who had their personal information collected by AddShoppers and whose online activity was tracked by AddShoppers (the "Class").

California subclass:

> All California residents who had their personal information collected by AddShoppers and whose online activity was tracked by AddShoppers (the "California Subclass").

71. The proposed classes expressly exclude persons who directly enrolled in the SafeOpt program operated by AddShoppers; any officers and directors of Defendants; Class Counsel; and the judicial officers presiding over this action and the members of their immediate family and judicial staff.

72. This action satisfies all the relevant requirements of Rule 23.

73. Members of the class and subclass are so numerous that their individual joinder is impracticable. On information and belief, members of the class and subclass number in the millions. The precise number of class members and their identities is unknown to Plaintiffs at this time but may be determined through discovery. Members of the class may be notified of the pendency of this action by mail or publication through the distribution records of Defendants.

74. Common questions of law and fact exist as to all members of the class and subclass and predominate over questions affecting only individual class members. Common legal and factual questions include but are not limited to whether Defendants have violated the California Invasion of Privacy Act (CIPA), Cal. Penal Code § 631, invaded class members' common law privacy rights, California's Unfair Competition Law, unjust enrichment and whether class members are entitled to actual or statutory damages for those violations.

75. Plaintiffs' claims are typical of the claims of the class because Plaintiffs, like all other members of the class, visited websites of members in the Data Co-Op and had their electronic communications intercepted and disclosed to AddShoppers through AddShoppers' illegal wiretaps.

76. Plaintiffs are adequate representatives of the class because their interests do not conflict with the interests of the members of the class they seek to represent, they have retained competent counsel experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of members of the class will be fairly and adequately protected by Plaintiffs and their counsel.

77. The class mechanism is superior to other available means for the fair and efficient adjudication of the class members' claims. Each individual class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendants' liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. By contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendants' liability. Class treatment of the liability issues will ensure that all claims and claimants are before this Court for consistent adjudication of the liability issues.

78. Plaintiffs bring all claims individually and on behalf of members of the class against Defendants.

**COUNT 1**
**Violation of the California Invasion of Privacy Act,**
**Cal. Penal Code § 631**
**(On behalf of the California subclass against Defendant AddShoppers and the Class against Defendants Peet's)[19]**

79. Plaintiffs repeat and reallege all preceding paragraphs.

80. Plaintiffs Lineberry and Cordero bring this claim individually and on behalf of the California subclass against Defendant AddShoppers. Plaintiffs Cook and Cordero brings this claim individually and on behalf of the Class against Defendant Peet's.

81. To establish liability under Cal. Penal Code Section 631(a), Plaintiffs need only establish that AddShoppers, "by means of any machine, instrument, contrivance, or in any other manner," did any of the following:

i. Intentionally taps, or makes any unauthorized connection, whether physically, electrically, acoustically, inductively or otherwise, with any telegraph or telephone wire, line, cable, or instrument, including the wire, line, cable, or instrument of any internal telephonic communication system;

ii. Willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads or attempts to read or learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line or cable or is being sent from or received at any place within this state;

iii. Uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained; or

iv. Aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section.

[19] Plaintiffs do not seek reconsideration of the Court's motion to dismiss ruling but include certain Counts in the amended complaint to preserve any appellate rights. *See* Dkt. No. 89

82. Section 631(a) applies to "new technologies" such as computers, the internet, and email.[20]

83. AddShoppers' software, including its SafeOpt service, is a "machine, instrument, contrivance, or . . . other manner" used to engage in the prohibited conduct here.

84. At all relevant times, by using AddShoppers' technology, AddShoppers willfully and without the consent of all parties to the communication, or in any unauthorized manner, read or attempted to read or learn the contents or meaning of electronic communications of Plaintiffs and putative class members, while the electronic communications were in transit or passing over any wire, line or cable or were being sent from or received at any place within California.

85. By embedding AddShoppers' technology on its website, Defendant Peet's aided, agreed with, employed, and conspired with AddShoppers to carry out the wrongful conduct alleged. *See* Cal. Penal Code § 31.

86. Plaintiffs and class members did not consent to any websites' actions in implementing AddShoppers' wiretaps on the websites. Nor have either Plaintiffs or class members consented to Defendants' intentional access, interception, reading, learning, recording, and collection of Plaintiffs' and class members' electronic communications.

87. Plaintiffs and class members seek all relief available under Cal. Penal Code § 637.2, including injunctive relief and statutory damages of $5,000 per violation.

[20] *See Matera v. Google Inc.*, 2016 WL 8200619, at *21 (N.D. Cal. Aug. 12, 2016) (CIPA applies to "new technologies" and must be construed broadly to effectuate its remedial purpose of protecting privacy); *Bradley v. Google, Inc.*, 2006 WL 3798134, at *5-6 (N.D. Cal. Dec. 22, 2006) (CIPA governs "electronic communications"); *In re Facebook, Inc. Internet Tracking Litigation*, 956 F.3d 589 (9th Cir. 2020) (reversing dismissal of CIPA and common law privacy claims based on Facebook's collection of consumers' Internet browsing history).

**COUNT 2**
**Violations of California Penal Code § 502,**
**Computer Access and Data Fraud Act (CDAFA)**
**(On behalf of the California subclass against Defendant AddShoppers and the Class against Defendants Peet's)**

88. Plaintiffs repeat and reallege all preceding paragraphs.

89. Plaintiffs Lineberry and Cordero bring this claim individually and on behalf of the California subclass against Defendant AddShoppers. Plaintiffs Cook and Cordero brings this claim individually and on behalf of the Class against Defendant Peet's.

90. AddShoppers violated Cal. Penal Code § 502(c)(2) by knowingly and without permission accessing, taking and using Plaintiffs' and the class members' personally identifiable information.

91. AddShoppers accessed, copied, used, made use of, interfered with, or altered data belonging to Plaintiffs and class members: (1) in and from the State of California; (2) in the states in which Plaintiffs and the class members are domiciled; and (3) in the states in which the servers that provided services and communication links between Plaintiffs and the class members and AddShoppers and other websites with which they interacted were located.

92. Cal. Penal Code § 502 provides: "For purposes of bringing a civil or a criminal action under this section, a person who causes, by any means, the access of a computer, computer system, or computer network in one jurisdiction from another jurisdiction is deemed to have personally accessed the computer, computer system, or computer network in each jurisdiction."

93. AddShoppers has violated California Penal Code § 502(c)(1) by knowingly and without permission altering, accessing, and making use of Plaintiffs and class members' personally identifiable data in order to execute a scheme to defraud consumers by using and profiting from

the sale of their personally identifiable data, thereby depriving them of the value of their personally identifiable data.

94. AddShoppers has violated California Penal Code § 502(c)(6) by knowingly and without permission providing, or assisting in providing, a means of accessing Plaintiffs' and class members' computer systems or computer networks.

95. AddShoppers has violated California Penal Code § 502(c)(7) by knowingly and without permission accessing, or causing to be accessed, Plaintiffs' and class members' computer systems or computer network.

96. Under California Penal Code § 502(b)(10), a "Computer contaminant" is defined as "any set of computer instructions that are designed to . . . record, or transmit information within computer, computer system, or computer network without the intent or permission of the owner of the information."

97. AddShoppers has violated California Penal Code § 502(b)(8) by knowingly and without permission introducing a computer contaminant into the transactions between Plaintiffs and the class members and websites; specifically, a "cookie" that intercepts and gathers information concerning Plaintiffs' and the class members' interactions with certain websites, which information is then transmitted back to AddShoppers.

98. By embedding AddShoppers' technology on its website, Defendants Peet's aided, agreed with, employed, and conspired with AddShoppers to carry out the wrongful conduct alleged. *See* Cal. Penal Code § 31.

99. As a direct and proximate result of AddShoppers' unlawful conduct under California Penal Code § 502, AddShoppers has caused loss to Plaintiffs and the class members in

an amount to be proven at trial. Plaintiffs and the class members are also entitled to recover their reasonable attorneys' fees pursuant to California Penal Code § 502(e).

100. Plaintiffs and the class members seek compensatory damages, in an amount to be proven at trial, and declarative or other equitable relief.

101. Plaintiffs and the class members are entitled to punitive or exemplary damages pursuant to Cal. Penal Code § 502(e)(4) because AddShoppers' violations were willful and, upon information and belief, AddShoppers is guilty of oppression, fraud, or malice as defined in Cal. Civil Code § 3294.

**COUNT 3[21]**
**Statutory Larceny**
**California Penal Code §§ 484 and 496**
**(On behalf of the California subclass against Defendant AddShoppers and the Class against Defendants Peet's)**

102. Plaintiffs repeat and reallege all preceding paragraphs.

103. Plaintiff Lineberry brings this claim individually and on behalf of the California subclass against Defendant AddShoppers. Plaintiff Cook brings this claim individually and on behalf of the Class against Defendant Peet's.

104. Section 496(a) prohibits obtaining property "in any manner constituting theft."

105. Section 484 defines theft, and provides:

> Every person who shall feloniously steal, take, carry, lead, or drive away the personal property of another, or who shall fraudulently appropriate property which has been entrusted to him or her, or who shall knowingly and designedly, by any false or fraudulent representation or pretense, defraud any other person of money, labor or real or personal property, or who causes or procures others to report falsely of his or her wealth or mercantile character and by thus imposing upon any person,

[21] The Court dismissed Counts 3 and 5-6 of this complaint on Defendants' motions to dismiss. *See* Dkt. No. 89. Plaintiffs do not seek reconsideration of this ruling but include these Counts to preserve any appellate rights.

> obtains credit and thereby fraudulently gets or obtains possession of money, or property or obtains the labor or service of another, is guilty of theft.

106. Section 484 therefore defines "theft" to include obtaining property by false pretense.

107. AddShoppers intentionally designed a program that would operate in a manner unbeknownst to Plaintiffs whose computers were thus deceived into providing personally identifiable information to Defendants.

108. By embedding AddShoppers' technology on its website, Peet's aided, agreed with, employed, and conspired with AddShoppers to carry out the wrongful conduct alleged. *See* Cal. Penal Code § 31.

109. AddShoppers acted in a manner constituting theft or false pretense.

110. AddShoppers stole, took, or fraudulently appropriated Plaintiffs' PII without their consent.

111. AddShoppers concealed, aided in the concealing, sold, or used Plaintiffs' PII that was obtained by Defendants for Defendants' commercial purposes and the financial benefit of Defendants.

112. AddShoppers knew that Plaintiffs' personal information was stolen or obtained in a manner that was concealed or withheld from Plaintiffs.

113. The reasonable and fair market value of the unlawfully obtained personal data can be determined in the marketplace.

**COUNT 4**
**Violation of California's Unfair Competition Law (UCL)**
**Cal. Bus. & Prof. Code §§ 17200, et seq.**
**(On behalf of the California subclass against Defendant AddShoppers)**

114. Plaintiffs repeat and reallege all preceding paragraphs.

115. Plaintiff Lineberry and Cordero bring this claim individually and on behalf of the California subclass against Defendant AddShoppers.

116. California Business and Professions Code section 17200 *et seq*. ("UCL") prohibits "unlawful, unfair, or fraudulent business acts or practices."

117. By selling or providing personal information and data without consent, as described above, AddShoppers engaged in unlawful and unfair acts and practices prohibited by the UCL.

118. AddShoppers' knowingly used and continues to use the PII of Plaintiffs and class members through SafeOpt to sell products for its clients. AddShoppers' use of this information is central to the SafeOpt program.

119. AddShoppers' appropriation of class members' PII was to its economic and commercial advantage. AddShoppers has generated substantial revenue from SafeOpt.

120. At no time have Defendants affirmatively sought consent from class members before appropriating and selling their PII.

121. Plaintiffs and class members received no compensation from Defendants use of their PII.

122. AddShoppers' use of Plaintiffs' and class members' PII is directly connected to SafeOpt's commercial purposes: SafeOpt would be without value if SafeOpt did not include class members' PII. Simply put, Plaintiffs' and class members' PII is the product.

123. AddShoppers' conduct constitutes unfair business practices under the UCL because these practices offend established public policy and hurt Plaintiffs and class members, which cannot be reasonably avoided, and that outweighs any benefit to consumers or competition. The

conduct also is immoral, unethical, oppressive, unscrupulous, and substantially injurious to consumers.

124. California's UCL allows anyone to bring an action for injunctive relief if they have "lost money or property as a result of the unfair competition." Cal. Bus. & Prof. § 17204.

125. Plaintiffs lost money or property because of AddShoppers' unfair and unlawful practices in violation of the UCL. If not for its violation of the law, AddShoppers would have paid Plaintiffs for consent to sell their information or ceased the sale of their information.

126. Plaintiffs' and class members' PII is likely to remain available through SafeOpt, without their consent, and without compensation from AddShoppers for its appropriation and sale of that information. Indeed, the longer SafeOpt is allowed to continue its practices the more information that it can unfairly and unlawfully collect as it adds more businesses to its growing network.

127. Plaintiffs seek an order to enjoin AddShoppers from such unlawful, unfair and fraudulent business acts or practices and to restore to Plaintiffs their interest in money or property that might have been acquired by AddShoppers through unfair competition.

**COUNT 5**
**Unjust Enrichment**
**(On behalf of the Class, or in the alternative, on behalf of the state subclasses against Defendant AddShoppers)**

128. Plaintiffs repeat and reallege all preceding paragraphs.

129. AddShoppers has wrongfully and unlawfully used Plaintiffs' and class members' PII without their consent for substantial profits.

130. Plaintiffs' and class members' PII have conferred an economic benefit on Defendants.

131. AddShoppers has been unjustly enriched at the expense of Plaintiffs and class members, and AddShoppers has unjustly retained the benefits of its unlawful and wrongful conduct.

132. It would be unequitable and unjust for AddShoppers to be permitted to retain any of the unlawful proceeds resulting from their unlawful and wrongful conduct.

133. Plaintiffs and class members are therefore entitled to equitable relief including restitution and disgorgement of all revenues, earnings, and profits that AddShoppers obtained as a result of their unlawful and wrongful conduct.

**COUNT 6**
**Common Law Invasion of Privacy/Intrusion**
**(On behalf of the Class, or in the alternative, on behalf of the state subclasses against all Defendants)**

134. Plaintiffs repeat and reallege all preceding paragraphs.

135. Plaintiffs bring this claim individually and on behalf of all class members against Defendants.

136. Plaintiffs and class members have an interest in: (1) precluding the dissemination or misuse of their sensitive, confidential PII; and (2) making personal decisions or conducting personal activities without observation, intrusion or interference, including, but not limited to, the right to visit and interact with various Internet sites without facing wiretaps without Plaintiffs' and class members' knowledge or consent.

137. As alleged above, AddShoppers intruded into a conversation in which Plaintiffs had a reasonable expectation of privacy. That intrusion occurred in a manner that was highly offensive to a reasonable person. AddShoppers gained unwanted access to data by electronic and covert means, in violation of the law and social norms.

138. At all relevant times, by implementing AddShoppers' wiretaps on the websites, each Defendant intentionally invade Plaintiffs' and class members' common law privacy rights and procured the other Defendants to do so.

139. Plaintiffs and class members had a reasonable expectation that their PII and other data would remain confidential, and that Defendants would not install wiretaps on the websites.

140. Plaintiffs and class members did not consent to any of Defendants' actions in implementing AddShoppers wiretaps on the websites.

141. The invasion of privacy is serious in nature, scope and impact.

142. The invasion of privacy alleged here constitutes an impermissible breach of social norms underlying the privacy right.

143. Plaintiffs and class members seek all relief available for common law invasion of privacy claims under the applicable state laws.

**PRAYER FOR RELIEF**

For all the reasons above, Plaintiffs request that the Court:

i. Certify this action as a class action for all counts;

ii. Appoint Plaintiffs as class representatives and appoint their attorneys as class counsel;

iii. Award injunctive relief;

iv. Award compensatory, nominal, punitive, and statutory damages in amounts to be determined by the Court or jury;

v. Issue an order for public injunctive relief under the UCL;

vi. Award reasonable attorneys' fees and costs;

vii. Award prejudgment interest on all amounts awarded; and

viii. Grant such further relief that the Court deems necessary and proper.

**DEMAND FOR TRIAL BY JURY**

Plaintiffs demand a trial by jury of all issues that are triable.

Dated: November 22, 2024

Respectfully submitted,

*/s/ Kasey A. Youngentob*

**STUEVE SIEGEL HANSON LLP**
Norman E. Siegel
J. Austin Moore
Kasey A. Youngentob

**GIBBS LAW GROUP LLP**
David M. Berger

*Attorneys for Plaintiffs*